SOC Incident Response Report

Prepared by: Amithabh D.K

Date: July 3, 2025

SIEM Tool Used: Splunk (Free Trial Version)

Executive Summary

On July 3, 2025, multiple security anomalies were detected across a simulated enterprise network, including malware infections, login anomalies, and suspicious file access. Using Splunk, the SOC team identified high-severity events across multiple systems, indicating compromised endpoints and potential insider or external threat activity. An incident response workflow was initiated to investigate, contain, and report the threats.

Incident Details

- Incident ID: IR-2025-002
- Detection Time: 3-July-2025, 06:10 IST
- Detection Source: SIEM Alert (Splunk)
- Affected Systems: Multiple endpoints (10.0.0.5, 198.51.100.42, 203.0.113.77, etc.)
- Business Impact: Risk of malware propagation and sensitive file exposure

Timeline of Events

→ 05:06:14 - Malware detected (Worm) on bob@203.0.113.77
→ 05:48:14 - Trojan activity on bob@10.0.0.5
→ 09:10:14 - Ransomware behavior on bob@172.16.0.3
→ 04:19:14 - Rootkit detected on alice@198.51.100.42
→ 04:41:14 - Spyware alert on alice@172.16.0.3
→ 09:07:14 - Unusual login success by eve@203.0.113.77 after failed attempts by david
→ 08:42:14 - Suspicious file accessed by charlie on infected system

Indicators of Compromise (IOC)

✓ Infected IPs: 10.0.0.5, 198.51.100.42, 172.16.0.3, 203.0.113.77
✓ Malware Types Detected: Trojan, Worm, Ransomware, Rootkit, Spyware
✓ Users Involved: bob, alice, charlie, david, eve
✓ Targeted Actions: Login attempts, file access, malware triggers

Incident Classification

- Type: Multi-Vector Malware & Suspicious Access
- Category: Category 2 - Threat to Confidentiality & Integrity
- Severity: High
- Threat Actor: Unknown (Internal/External - Simulated Data)

Root Cause Analysis

The infections were primarily caused by poor endpoint hygiene and lack of access control. Login anomalies indicate potential credential misuse or phishing. Post-infection file access patterns suggest possible data exfiltration or malware-triggered events. MFA was not enforced and audit trails lacked early alerts.

Forensic Investigation

- Analyzed Splunk event logs (actions: login failed/success, malware detected, file accessed)
- Correlated activity across users and timestamps
- Detected repeat access from suspicious IPs after malware detections
- Verified no lateral movement between servers due to segmentation in simulation

Remediation Actions

- ✓ Blocked IPs: 10.0.0.5, 203.0.113.77, 198.51.100.42
- ✓ Reset passwords for affected users
- ✓ Deployed anti-malware tools on all endpoints
- ✓ Enabled MFA across all accounts
- ✓ Reviewed and tightened file access permissions
- ✓ Created new Splunk rules for faster anomaly detection

Damage and Cost Assessment

- Data Exposure: Risk of unauthorized access to internal files
- Data Loss: None confirmed (simulated environment)
- Estimated Cost: ~$5,000 (based on analyst hours + remediation in real scenario)

Lessons Learned and Recommendations

- Enforce MFA and strong password policies
- Implement stricter file access control
- Monitor and block IPs with high alert frequency
- Regularly update and test incident response playbooks
- Conduct quarterly red team assessments and phishing simulations

Evidence Preservation

- ❖ Archived Splunk queries and dashboards
- ❖ Exported logs showing malware and login events
- ❖ Saved screenshots of event timelines
- ❖ Documented session data for future auditing